ABSTRACT OF THE DISCLOSURE

An exponent calculation apparatus calculates x^e based on input two integers x and e. A pre-calculation module pre-calculates x^{l_i} for each of candidate exponents {l_i} ($0 \leq i \leq L-1$) stored in a candidate exponents storing unit, the number of the candidate exponents being L, and stores the obtained values x^{l_i} in a pre-calculated values storing unit. A dividing module divides the integer e into a plurality of values {f_i} ($0 \leq i \leq F-1$) so that each of the values {f_i} corresponds to one of the candidate exponents {l_i}. A sequential processing module sequentially updates a calculation result c, which is stored in a calculation result storing unit, for each of the values {f_i} by using each of the values x^{l_i}. The updated calculation result c for each of the values {f_i} is output as x^e. Accordingly, the amount of pre-calculation and table size can be reduced and thus the number of calculations can be reduced.